CLAIMS

What is claimed is:

1. A method for facilitating secure communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of:

receiving, from a first node, a first request to store an encryption key, wherein the first request includes an identifier, and wherein the first node uses the encryption key to encrypt data that is multicast with the identifier to a plurality of second nodes;

in response to the first request,

storing the encryption key;

creating and storing an association between the encryption key and the identifier;

receiving, from at least one second node of the plurality of second nodes, a second request to obtain the encryption key, wherein the second request includes the identifier;

in response to the second request,

based on the identifier included in the second request and the association between the encryption key and the identifier, retrieving the encryption key; and

sending the encryption key to the at least one second node for use in decrypting the encrypted data.

2. A method as recited in Claim 1, wherein:

a trusted third party performs the steps of receiving the first request, storing the encryption key, creating and storing the association, receiving the second request, retrieving the encryption key, and sending the encryption key;

the first node is a router that acts as a multicast originator; and

the plurality of second nodes is a plurality of routers that act as multicast receivers.

3. A method as recited in Claim 2, wherein the trusted third party is selected from the group consisting of a certificate authority, a key distribution center, a key exchange authority, and a key exchange center.

4. A method as recited in Claim 1, wherein the step of receiving the first request includes the step of:
receiving a third request to register the encryption key and the identifier.

5. A method as recited in Claim 1, wherein the steps of creating and storing the association include the step of:
registering a certificate that includes the encryption key and the identifier.

6. A method as recited in Claim 5, further comprising the computer-implemented steps of:
in response to the first request, associating an expiration time with the encryption key;
in response to the second request, determining based on the expiration time whether the encryption key has expired; and
when the encryption key has expired, revoking the certificate.

7. A method as recited in Claim 1, further comprising the computer-implemented steps of:
in response to the first request, associating an expiration time with the encryption key;
in response to the second request, determining based on the expiration time whether the encryption key has expired; and
when the encryption key has not expired, performing the steps of retrieving and sending the encryption key.

8. A method as recited in Claim 1, further comprising the computer-implemented steps of:
registering the first node; and
registering one or more nodes of the plurality of second nodes.

9. A method as recited in Claim 1, further comprising the computer-implemented steps of:

generating the encryption key based on an Internet key exchange protocol with the first node.

10. A method as recited in Claim 1, wherein the encryption key is selected from the group consisting of a private key, a shared key, a pseudo-random string of bits, and a pseudo-random string of characters.

11. A method as recited in Claim 1, wherein:

the first node uses the encryption key and Internet protocol security (IPsec) to encrypt the data that is multicast; and

the at least one second node decrypts the encrypted data based on the encryption key and IPsec.

12. A method as recited in Claim 1, wherein the first request includes a list of authorized second nodes, and further comprising the computer-implemented steps of:

in response to the first request, storing the list of authorized second nodes;

in response to the second request, determining whether the at least one second node is included in the list of authorized second nodes; and

when the at least one second node is included in the list of authorized second nodes, performing the steps of retrieving and sending the encryption key.

13. A method as recited in Claim 1, further comprising the computer-implemented steps of:

storing a list of nodes;

in response to the first request, determining whether the first node is included in the list of nodes;

when the first node is included in the list of nodes, performing the steps of storing the encryption key and creating and storing the association between the encryption key and the identifier.

14. A method as recited in Claim 1, further comprising the computer-implemented steps of:

in response to the first request, associating one or more criteria with the encryption key;

in response to the second request, determining based on the one or more criteria whether the encryption key is valid; and

when the encryption key is valid, performing the steps of retrieving and sending the encryption key.

15. A method as recited in Claim 1, wherein the encryption key is an old encryption key, the identifier is an old identifier, and the association is an old association, and further comprising the steps of:

in response to the first request, associating one or more criteria with the encryption key;

in response to the second request, determining based on the one or more criteria whether the encryption key is valid; and

when the encryption key is not valid,

receiving a third request to store a new encryption key, wherein the third request includes a new identifier, and wherein the new encryption key is used to encrypt additional data that is multicast with the new identifier to the plurality of second nodes;

in response to the third request,

storing the new encryption key;

creating and storing a new association between the new encryption key and the new identifier;

receiving, from at least one additional second node of the plurality of second nodes, a fourth request to obtain the new encryption key, wherein the fourth request includes the new identifier;

in response to the fourth request,

based on the new identifier included in the fourth request and the new association between the new encryption key and the new identifier, retrieving the new encryption key; and

sending the new encryption key to the at least one additional second node for use in decrypting the encrypted data.

16. A method as recited in Claim 1, wherein the data that the first node encrypts and multicasts is received from a source node.

17. A method as recited in Claim 1,

wherein:

the identifier is a session identifier;

the encrypted data is multicast with an originator identifier that is based on an identity of the first node;

the second request includes an unverified originator identifier; and

further comprising the computer-implemented steps of:

in response to the first request, associating the originator identifier with the session identifier; and

in response to the second request, determining whether the unverified originator identifier is valid based on the originator identifier and informing the at least one second node whether the unverified originator is valid.

18. A method as recited in Claim 1, wherein:

a trusted third party performs the steps of receiving the first request, storing the encryption key, creating and storing the association, receiving the second request, retrieving the encryption key, and sending the encryption key;

the first request is encrypted based on a public key that is associated with the trusted third party; and

the first request is signed with a private key that is associated with the first node.

19. A method as recited in Claim 1, wherein a trusted third party performs the steps of receiving the first request, storing the encryption key, creating and storing the association, receiving the second request, retrieving the encryption key, and sending the encryption key, and further comprising the computer-implemented steps of:

prior to sending the encryption key,

encrypting the encryption key based on a public key that is associated with the at least one second node; and

signing the encrypted encryption key with a private key that is associated with the trusted third party.

20. A method as recited in Claim 1, wherein the identifier is selected from the group consisting of a hostname, an Internet protocol address, a media access control address, an Internet security protocol security parameter index, a first string of pseudo-random bits, a second string of pseudo-random characters, a third string of arbitrary bits, and a fourth string of arbitrary characters.

21. A method for encrypting communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of:

sending an encryption key and an identifier that is associated with the encryption key to an authoritative node that stores the encryption key and identifier and that creates and stores an association between the encryption the encryption key and the identifier;

encrypting data based on the encryption key; and

multicasting the encrypted data with the identifier to one or more receiving nodes, wherein the one or more receiving nodes use the identifier to retrieve the encryption key from the authoritative node and decrypt the encrypted data based on the encryption key.

22. A method for decrypting encrypting communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of:

receiving from an originating node a multicast that includes encrypted data and an identifier;

identifying the identifier from the multicast;

sending a request that includes the identifier to an authoritative node for an encryption key used by the originating node to encrypt the encrypted data;

in response to the request to the authoritative node, receiving the encryption key; and

decrypting the encrypted data based on the encryption key.

23. A method for a certificate authority to facilitate communications based on Internet protocol security (IPsec) among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of:

receiving, at the certificate authority from a first router that acts as a multicast originator, a first request to register an encryption key, wherein the first request includes a multicast session identifier and a list of authorized multicast receivers, and wherein the first router uses the encryption key to encrypt data based on IPsec and multicasts the encrypted data with the multicast session identifier to a plurality of second routers that act as multicast receivers;

in response to the first request, the certificate authority creating and storing a multicast session certificate that includes the encryption key, the multicast session identifier, and the list of authorized multicast receivers;

receiving, at the certificate authority from at least a particular second router of the plurality of second routers, a second request to obtain the encryption key, wherein the second request includes the multicast session identifier;

in response to the second request,

determining whether the particular second router is included in the list of authorized multicast receivers;

when the particular second router is included in the list of authorized multicast receivers, based on the multicast session identifier included in the second request and the multicast session certificate, the certificate authority retrieving the encryption key; and

the certificate authority sending the encryption key to the particular second router for use in decrypting the encrypted data based on IPsec.